UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

SHERRI ADDISON, Individually and on Behalf of All Others Similarly Situated, Plaintiff, vs. CROUSE HEALTH HOSPITAL, INC. and PERRY JOHNSON & ASSOCIATES, INC., Defendants.	Case No. 1:24-CV-782 (AMN/CFH) **COMPLAINT** **CLASS ACTION** **DEMAND FOR JURY TRIAL**

Sherri Addison ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Crouse Health Hospital, Inc., d/b/a Crouse Hospital ("Crouse") and Perry Johnson & Associates, Inc. ("PJ&A," collectively with Crouse, "Defendants") seeking monetary damages, restitution, and/or injunctive relief for herself and the proposed Class and New York Subclass, as defined *infra*. Plaintiff makes the following allegations upon personal knowledge as to her actions and on information and belief derived from, *inter alia*, the investigation of her counsel and facts that are a matter of public record.

NATURE OF THE ACTION

1. On or about December 8, 2023, PJ&A sent Plaintiff and other members of the Class and New York Subclass a "Notice of Data Breach" (the "Notice"). The Notice provided, among other things, that "[o]n May 2, 2023, PJ&A became aware of a potential data security incident impacting PJ&A's systems." According to the Notice, "[o]n May 22, 2023, we preliminarily determined that an unauthorized third party had accessed PJ&A data and that customer data was likely impacted by this event, although further investigation would be required to determine the scope of the impacted data and to identify all affected customers." PJ&A "determined that the

unauthorized access to [its] systems occurred between March 27, 2023, and May 2, 2023, and the unauthorized access to personal health information, including information pertaining to certain Crouse patients, occurred between April 7, 2023, and April 19, 2023, with certain subsets of data accessed for shorter periods during this timeframe." The incident, occurring from at least April 7, 2023, through at least April 19, 2023, is referred to herein as the "Data Breach." The Notice does not provide when Crouse learned of the Data Breach.

2. On November 3, 2023, PJ&A notified the U.S. Department of Health and Human Services (the "HHS") that 8,952,212 individuals were affected by the Data Breach.[1]

3. According to the "Statement From Crouse Health Regarding PJ&A Data Breach," dated December 12, 2023, "Perry Johnson & Associates (PJ&A), a medical transcription service assisting providers across the U.S., has experienced a data breach as a result of a hacking incident in its own systems. At least 4 million New Yorkers have been impacted by the data breach, including some (but not all) Crouse Health patients."[2]

4. Defendant Crouse has been in operation since 1887. According to its website, "Crouse is licensed for 506 acute-care adult beds and 57 bassinets, and serves more than 23,000 inpatients, 56,000 emergency services visits and more than 600,000 outpatients a year from a 16-county area in Central and Northern New York."[3]

5. According to the Notice, Defendant PJ&A provides certain medical transcription and related services to Crouse. As provided in a fact sheet issued by HHS, PJ&A is a Business

[1] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed on June 7, 2024).

[2] *See* https://www.crouse.org/news/statement-pja-data-breach/ (last accessed on June 7, 2024).

[3] *See* https://www.crouse.org/about/ (last accessed on June 7, 2024).

Associate of Crouse under Healthcare Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1320d, *et seq*.[4]

6. Defendants' computer systems contained Personal Identifiable Information ("PII") and Personal Health Information ("PHI", collectively with PII, "Private Information") of nearly nine million people affected by the Data Breach. According to the Federal Trade Commission ("FTC"), PII is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[5] PHI is deemed private under the HIPAA, as well as multiple state statutes. According to the HHS, PHI "is information, including demographic data, that relates to: [ ] the individual's past, present or future physical or mental health or condition, [ ] the provision of health care to the individual, or [ ] the past, present, or future payment for the provision of health care to the individual, [ ] and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual."[6]

7. According to the Notice, the information on PJ&A's computer systems included Plaintiff and the Class and New York Subclass's names, dates of birth, addresses, phone numbers, sex, medical record numbers, health insurance information, dates of admission and discharge, attending physician identifiers, hospital room numbers, and visit types. Additionally, for a small

[4] *See Business Associates*, HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html (last accessed on June 7, 2024).

[5] *See Federal Trade Commission Privacy Impact Assessment: Redress Enforcement Database (RED)* at 3 n.3, FTC (June 2019), https://www.ftc.gov/system/files/attachments/privacy-impact-assessments/redress_enforcement_database_red_privacy_impact_assessment_june_2019.pdf.

[6] *See Summary of the HIPAA Privacy Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed on June 7, 2024).

fraction of Crouse patients, the data accessed may have included a transcript of care dictated by the patient's physician.

8. During the Data Breach, unauthorized actors had unfettered access to Plaintiff and the other members of the Class and New York Subclass's Private Information.

9. Plaintiff and other members of the Class and New York Subclass provided their Private Information to Crouse, and Crouse then provided that Private Information to PJ&A, Crouse's Business Associate.

10. PJ&A inadequately maintained its computer systems, rendering them—and Plaintiff and the Class and New York Subclass's Private Information—easy prey for cyber theft.

11. Upon information and belief, PJ&A was on notice that its inadequate data security created a heightened risk for cyber theft.

12. Crouse separately had a duty to maintain the security of Plaintiff and the other members of the Class and New York Subclass's Private Information, and to ensure that its HIPAA Business Associate, PJ&A, had adequate and reasonable data security in place to safeguard Private Information and comply with HIPAA. Upon information and belief, Crouse failed to satisfy those duties.

13. After the Data Breach, PJ&A and Crouse failed to provide timely notice to the affected Plaintiff and the other members of the Class and New York Subclass – thereby exacerbating their injuries. Ultimately, PJ&A and Crouse deprived Plaintiff and other members of the Class and New York Subclass of the chance to take speedy measures to protect themselves and mitigate harm.

14. Moreover, when PJ&A ultimately notified Plaintiff and other members of the Class and New York Subclass of the exfiltration of Private Information, PJ&A failed to adequately describe the Data Breach and its effects.

15. Plaintiff and the other members of the Class and New York Subclass's identifying information is compromised and already in imminent jeopardy – all because of PJ&A and Crouse's negligence. Members of the Class and New York Subclass have already been victimized by identity theft and fraud by virtue of the Data Breach and, as a result, Plaintiff and all members of the Class and New York Subclass now suffer from a heightened and imminent risk of fraud and identity theft and must now constantly monitor their financial and medical accounts.

16. The disclosure of a person's Private Information can be devastating and, the longer the data is lost, the worse the injury may become. Not only is it an intrusion of privacy and a loss of control, but it is also a harbinger of identity theft: for victims of a data breach, the risk of identity theft more than quadruples.[7] A data breach can have grave consequences for victims for many years after the actual date of the breach – with the obtained information, identity thieves can wreak many forms of havoc, including, but not limited to, opening new financial accounts and obtaining medical services, government benefits, or driver's licenses in the victims' names – forcing victims to maintain a constant vigilance over the potential misuse of their information.

17. As a result of the Data Breach, Plaintiff and the other Class and New York Subclass members have and will suffer ascertainable losses. Plaintiff and other members of the Class and New York Subclass have suffered, and will continue to suffer, from the loss of the benefit of their bargain with Crouse, unexpected out-of-pocket expenses, diminished value of their Private

[7] Dave Maxfield & Bill Latham, *Data Breaches: Perspectives from Both Sides of the Wall*, S.C. Law (May 2014).

Information, and the value of their time reasonably incurred to mitigate the fallout of the Data Breach.

18. Plaintiff seeks to remedy these injuries on behalf of herself and all similarly situated individuals whose Private Information was compromised in the Data Breach.

19. Plaintiff brings this proposed class action lawsuit to address, *inter alia*, Defendants' failure to: (1) safeguard the Class and New York Subclass members' Private Information, which Defendants procured and maintained on their computer systems; (2) provide timely and adequate notice to Plaintiff and the other Class and New York Subclass members that their information had been subject to the unauthorized access by an unknown third-party; and (3) provide Plaintiff and the other Class and New York Subclass members with adequate redress for the Data Breach or act to mitigate their damages.

20. Plaintiff seeks remedies, including, but not limited to, compensatory damages, statutory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief, including improvements to PJ&A and Crouse's computer systems, future annual audits, and adequate credit monitoring services funded by PJ&A and Crouse.

PARTIES

21. Plaintiff Sherri Addison is a citizen of New York, residing in Queensbury, Warren County, New York. Plaintiff received the Notice via U.S. Mail in December 2023.

22. Defendant Crouse Health Hospital, Inc., d/b/a Crouse Hospital, is a New York not-for-profit corporation headquartered at 736 Irving Avenue, Syracuse, New York 13210.

23. Defendant Perry Johnson & Associates, Inc. is a Nevada corporation which provides on its website that it is located at 1489 West Warm Springs Road, Suite 110, Henderson,

Nevada, 89012.[8] In a filing before the U.S. Judicial Panel on Multidistrict Litigation, PJ&A represented that its principal place of business is located at 755 W. Big Beaver Road, #1300, Troy, Michigan 48084. *See In re Perry Johnson & Assocs. Med. Transcription Data Sec. Breach Litig.*, Case No. 3096 (J.P.M.L. Jan. 4, 2024), Dkt. 86. Pursuant to HIPAA, Defendant PJ&A is a Business Associate of Defendant Crouse.

JURISDICTION AND VENUE

24. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d) because Plaintiff and at least one member of the Class is a citizen of a state that is diverse from at least one of the Defendants' citizenships, a class action has been pled, and the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs.

25. This Court has personal jurisdiction over Defendants because they regularly conduct business within this District. Furthermore, Defendant Crouse resides and operates in this District. Defendant PJ&A contracted with Crouse to act as a Business Associate and regularly does and solicits business within this District, and reasonably should have expected that its tortious acts would have consequences within this District.

26. Venue is proper in this District under 28 U.S.C. §1391 (a), (b), and (c); 28 U.S.C. §1407; and 15 U.S.C. §22 because Crouse has its principal place of business in this District and a substantial part of the events giving rise to Plaintiff's claim arose in this District.

FACTUAL ALLEGATIONS

27. Upon information and belief, in the course of providing medical care to Plaintiff and other members of the Class and New York Subclass, Crouse received and maintained Plaintiff

[8] *See* https://www.pjats.com/about-pja/ (last accessed on June 7, 2024).

and the Class and New York Subclass's PII and PHI. These records are stored on Crouse's and its Business Associates', including PJ&A's, computer systems.

28. Upon information and belief, in the course of providing medical care to Plaintiff and the other members of the Class and New York Subclass, health care providers employed by Crouse take notes that include PII and PHI relating to their individual medical conditions and treatments. Those raw notes are then transmitted to PJ&A, a Business Associate, to be transcribed into electronic medical records.

29. Because of the highly sensitive and personal nature of the information Crouse acquires and stores, Crouse and PJ&A knew or reasonably should have known that they must comply with healthcare industry standards related to data security and all federal and state laws and regulations protecting Private Information and providing adequate notice to customers if their Private Information is disclosed without proper authorization.

Crouse Failed to Comply with its own Privacy Policies

30. Because of the highly sensitive and personal nature of Plaintiff's Private Information that Crouse collects, Crouse has publicly affirmed its obligation and duty to secure Plaintiff's data, and the obligation and duty of its Business Associates, including PJ&A to secure Plaintiff's data.

31. Indeed, on its website, Crouse provides its *Notice of Privacy Practices*,[9] dated March 1, 2003, as revised in September 2013 ("Crouse's Privacy Practices"). Crouse's Privacy Practices state, in part:

> Crouse Hospital is required by law to protect the privacy of your health information. We must provide you with a copy of this Notice which describes our legal duties and privacy practices and your rights concerning your health information. The following

[9] *See* https://www.crouse.org/wp-content/uploads/2018/03/Notice-of-PrivacyREV09-13.pdf.

individuals at Crouse Hospital will follow this Notice when they provide services to you:

- Our medical staff, affiliated health professionals, and students;

- Our employees, personnel or representatives in every department having access to your health information;

- Our affiliates, including independent contractors having access to your health information.

Crouse Hospital and the above individuals may share your health information with each other as may be necessary to provide you treatment, for payment of your treatment, or to support our healthcare operations to the extent authorized by law.

Crouse Hospital is required to notify you of a breach of unsecured protected health information

32. According to Crouse's Privacy Practices:

WHAT HEALTH INFORMATION IS PROTECTED

Crouse Hospital is committed to protecting the privacy of your health information. Some examples of protected health information are:

- Information about your health condition (such as a disease you may have);

- Information about health care services you have received or may receive in the future (such as an operation);

- Information about your health care benefits under an insurance plan (such as whether a prescription is covered);

- Geographic information (such as where you live or work);

- Demographic information (such as your race, gender, ethnicity, or marital status);

- Unique numbers that may identify you (such as your social security number, your phone number, or your driver's license number); and

• Other identifying information. [10]

33. Furthermore, Crouse's *Corporate Compliance Program Handbook*[11] adopted on November 29, 1999, and revised in May 2023, provides, in part:

> **Confidentiality**
>
> Crouse Hospital has in its possession a broad variety of confidential, sensitive and proprietary information, which if inappropriately released, could be harmful to individuals, our business partners and to Crouse Hospital itself. Therefore, affected individuals should always safeguard confidential information concerning patients, employees, and business matters in accordance with Crouse Hospital's policies and procedures and relevant state and federal law. Each affected individual must always respect and maintain the privacy of confidential information, even after they are no longer affiliated with Crouse Hospital.
>
> Affected individuals should become familiar with their department's specific policies and procedures in addition to hospital-wide policies, such as the Notice of Privacy Practices as required by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").
>
> * * * * *
>
> Crouse Hospital will protect the confidentiality of patient information. Protected Health Information, or PHI, includes information such as: names, addresses, medical diagnoses, social security numbers, etc. HIPAA also requires adherence to the minimum necessary standard for use and disclosure of patient information.

34. The *Crouse Health Policy & Procedure*[;] *Confidentiality & Privacy*,[12] effective July 28, 2022, provides, in part, that:

> It is the policy of Crouse Hospital to protect and maintain the privacy and confidentiality of patient information and that all interactions with patients are strictly confidential. Such interactions

[10] *Id.*

[11] *See* https://www.crouse.org/wp-content/uploads/2023/06/Corporate-Compliance-Handbook.pdf at 10.

[12] *See* https://www.crouse.org/wp-content/uploads/2024/05/Confidentiality-Privacy-Policy.pdf.

> include but are not limited to the medical record, billing information and verbal or written discussions about patients. The only exception to this policy is when Federal or State law specifically allows the release of such interactions.

35. The *Crouse Health Policy & Procedure*[;] *HIPPA – Business Associates Uses & Disclosures*,[13] effective February 8, 2023 ("2023 Crouse's 2023 Business Associates Disclosure Policy") stated that it applies to "[a]ll individuals who work with third-party vendors/organizations that may access, store, create, alter, or remove Crouse Hospital patient data." It defined a "Business Associate" as "[a] person (non-employee) or entity that provides services, or performs functions, to a covered entity that involves access by the person/entity to protected health information."[14]

36. Crouse's 2023 Business Associates Disclosure Policy provided, in part, that:

> It is the policy of Crouse Hospital to ensure that any potential Business Associate that may access, transmit, and store electronic Protected Health Information (ePHI) of Crouse Hospital follow HIPAA Security safeguards and requirements when using and disclosing ePHI.
>
> Crouse Hospital will enter into a Business Associate Agreement (BAA) if the Business Associate accesses Hospital ePHI in any manner as per their functions and/or services. The BAA between the Business Associate and Crouse Hospital must indicate that the Business Associate will use the necessary administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of Crouse Hospital ePHI as required by the HIPAA Security Rule (45 CFR 164.302 through 164.318) and HIPAA Privacy Rule (45 CFR 162.502, 162.504).

* * * * *

[13] *See* https://www.crouse.org/wp-content/uploads/2023/02/HIPAA-Business-Associates-Uses-and-Disclosures-Polilcy.pdf. Crouse's 2023 Business Associates Disclosure Policy was updated after the Data Breach on February 5, 2024. *See* https://www.crouse.org/wp-content/uploads/2024/05/HIPAA-Business-Associates-Uses-and-Disclosures-Policy.pdf.

[14] *See* https://www.crouse.org/wp-content/uploads/2024/05/HIPAA-Business-Associates-Uses-and-Disclosures-Policy.pdf at 1, 3.

> Crouse Hospital reserves the right to terminate any BAA if the Hospital determines that the Business Associate has violated a term within the contract and/or HIPAA and the Business Associate has not taken steps to cure the violation. Refer to the HIPAA BAA (Doc #7564) for more information. [15]

37. Crouse's 2023 Business Associates Disclosure Policy further provided, in part, that:

> **Business Associate Agreement Requirements**
>
> Prior to allowing any Business Associate access to Hospital ePHI, Crouse Hospital must obtain assurance from the Business Associate that it will protect Hospital ePHI in the form of a written agreement. The agreement will include the following provisions:
>
> - Business Associates will comply with all provisions of HIPAA Security Rule (45 CFR 164.302 through 164.318) and all provisions of the HIPAA Privacy Rule (45 CFR 162.502, 162.504).
>
> - Protected Health Information will not be used or further disclosed other than as permitted or required by the contract or law.
>
> - The business associate will use appropriate safeguards to prevent use or disclosure of the information other than as provided in the contract.
>
> * * * * *
>
> Failure to follow any of these provisions could result in the potential unlawful disclosure or breach of Crouse Hospital ePHI. [16]

38. By obtaining, collecting, receiving, and/or storing Plaintiff and other members of Class and New York Subclass's Private Information, Crouse and PJ&A assumed legal and equitable duties and knew or should have known that they were responsible for protecting that Private Information from unauthorized disclosure.

---

[15] *See id* at 1.

[16] *See id.* at 1-2.

39. Plaintiff and the other members of the Class and New York Subclass have taken reasonable steps to maintain the confidentiality of their Private Information, including, but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

40. Upon information and belief, Plaintiff and the other members of the Class and New York Subclass relied on Crouse and its Business Associates, such as PJ&A, to keep their Private Information confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

41. PJ&A could have prevented or mitigated the effects of the Data Breach by better securing its computer systems and complying with HIPAA.

42. Crouse could have prevented or mitigated the effects of the Data Breach by ensuring that PJ&A had appropriate data security measures in place, or better selecting its Business Associates given access to Private Information.

43. According to the HSS, in a news release issued less than just over a month prior to the Notice, over eight-eight (88) million individuals were affected by large breaches of personal health information during the first ten (10) months of 2023 alone. This is a sixty percent (60%) increase in the number of individuals affected in 2022.[17]

44. The HSS further reported that "[i]n the past four years, there has been a 239% increase in large breaches reported to OCR involving hacking and a 278% increase in ransomware.

[17] *See* HSS, *HHS' Office for Civil Rights Settles Ransomware Cyber-Attack Investigation* (Oct. 31, 2023), https://www.hhs.gov/about/news/2023/10/31/hhs-office-civil-rights-settles-ransomware-cyber-attack-investigation.html (last accessed on June 7, 2024).

This trend continues in 2023, where hacking accounts for 77% of the large breaches reported to OCR."[18]

45. Despite the prevalence of public announcements of data breaches and data security compromises, Crouse and PJ&A failed to take appropriate steps to protect Plaintiff and the other members of Class and New York Subclass's Private Information from being compromised. Among other things:

a. Crouse and PJ&A failed to ensure risk analysis and risk management were properly integrated into PJ&A's business processes;

b. Crouse and PJ&A failed to properly conduct risk analysis and risk management regularly and when new technologies and business operations were planned;

c. Crouse and PJ&A failed to properly ensure PJ&A had adequate audit controls in place to record and examine information system activity;

d. Crouse and PJ&A failed to properly implement regular review of information system activity;

e. Crouse and PJ&A failed to properly utilize multi-factor authentication to ensure only authorized users were accessing the Private Information;

f. Crouse and PJ&A failed to ensure that Private Information was properly encrypted to guard against unauthorized access to the Private Information;

g. Crouse and PJ&A failed to ensure that training specific to organization and job responsibilities was properly provided and on a regular basis and that

[18] *Id.*

workforce members' critical role in protecting privacy and security was reinforced; and

h. Crouse failed to properly monitor PJ&A to ensure PJ&A had adequate safety and risk management procedures in place.

46. Furthermore, Crouse and PJ&A failed to timely and accurately disclose that Plaintiff and other members of the Class and New York Subclass's PII and PHI had been improperly acquired or accessed.

47. Indeed, the Data Breach was not disclosed to Plaintiff and other members of the Class and New York Subclass for more than seven (7) months after PJ&A became aware of the Data Breach. Notably, the *Crouse Health Policy & Procedure*[;] *HIPAA: Notification Process for Unsecured PHI Breach*,[19] effective September 27, 2019, requires that Crouse's Business Associates, such as PJ&A, notify Crouse of any data breach within sixty (60) days from the date of the discovery. That policy states, in part:

> **Business Associate Responsibilities:**
>
> A Business Associate is anyone who creates, receives, maintains or transmits PHI on behalf of Crouse Hospital. They are required to notify Crouse of any breach of unsecured PHI without unreasonable delay but ***no later than 60 days from the date of discovery*** or by the shorter timeframe specified in the Business Associate Agreement. The notice shall include the identification of each individual whose unsecured PHI has been accessed, acquired, or disclosed. The Business Associate shall promptly provide Crouse with any other available information required for the notification. Upon notification by the Business Associate of discovery of a breach, Crouse will be responsible for notifying affected individuals, unless otherwise agreed upon by the Business Associate to perform the notification. [Emphasis added.[20]]

[19] *See* https://www.crouse.org/wp-content/uploads/2024/05/HIPAA-Information-System-Activity-Review-Policy.pdf.

[20] *See id.* at 4.

The Data Breach

48. On or about December 8, 2023, PJ&A sent Plaintiff and other members of the Class and New York Subclass the Notice. The Notice provided, in part:

> **What Happened?** On May 2. 2023. PJ&A became aware of a potential data security incident impacting PJ&A's systems. Thereafter, we immediately launched an internal investigation and retained an external cybersecurity vendor to assist with the investigation, contain the threat and further secure our systems. On May 22, 2023, we preliminarily determined that an unauthorized third party had accessed PJ&A data and that customer data was likely impacted by this event, although further investigation would be required to determine the scope of the impacted data and to identify all affected customers. ***There was no compromise of Crouse's own systems. This incident occurred in PJ&A's environment only.***
>
> The investigation ultimately determined that the unauthorized access to PJ&A's systems occurred between March 27, 2023, and May 2, 2023, and that unauthorized access to personal health information, including information pertaining to certain Crouse patients, occurred between April 7, 2023, and April 19, 2023, with certain subsets of data accessed for shorter periods during this timeframe. PJ&A directed its external vendor to analyze the data and provide data sets that would identify all affected customers, individuals, and data elements. Working with Crouse, we were able to identify a list of patients whose information was involved in the incident over the past few weeks.
>
> **What Information Was Involved?** We have confirmed that a database containing some of your personal health information was accessed during this incident. Specifically, the PJ&A files that were accessed by the unauthorized third party contained information about you and certain other Crouse patients that may have included: first and last name, date of birth, address, sex, phone number, medical record number, health insurance information, dates of admission and discharge, attending physician identifiers, hospital room number, and visit type. For a small fraction of the patients whose data was accessed (<10%), it may also have included a transcript of care dictated by the patient's physician. ***Based on our analysis to date, the accessed data did <u>not</u> include your Social Security number or any bank account or credit card number.***

49. Although the Data Breach allegedly began on March 27, 2023, according to the Notice, PJ&A did not become aware of the unauthorized access of its computer systems until over a month later on May 2, 2023.

50. Upon information and belief, Plaintiff and the Class and New York Subclass's Private Information was accessed, exfiltrated, and stolen in the Data Breach.

51. Upon information and belief, the Private Information accessed during the Data Breach was unencrypted.

52. It is likely PJ&A was targeted in the Data Breach because it provides transcription services to healthcare providers that collect, create, and maintain both PII and PHI.

53. While the Notice provides that PJ&A became aware of the Data Breach as early as May 2, 2023, PJ&A did not begin notifying the Class and New York Subclass members of the Data Breach until over seven months later, on or after December 8, 2023.

54. Notably, the Notice fails to inform Plaintiff and the other members of the Class and New York Subclass when Crouse became aware of the Data Breach.

55. Time is of the essence when highly sensitive Private Information is subject to unauthorized access and/or acquisition. Plaintiff and the Class and New York Subclass's Private Information is believed to be available on the dark web where hackers can offer for sale unencrypted, unredacted Private Information to other criminals. Plaintiff and the Class and New York Subclass are now subject to the present and lifetime risk of fraud, identity theft, and misuse resulting from the publication and sale of their Private Information.

56. Following the Data Breach and recognizing that Plaintiff and each member of the Class and New York Subclass is now subject to the present and lifetime risk of identity theft and fraud. Indeed, in the Notice PJ&A advised Plaintiff and the Class and New York Subclass "to

remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your free credit reports for suspicious activity and to detect errors."

57. Crouse and PJ&A largely put the burden on Plaintiff and the Class and New York Subclass to take measures to protect themselves.

58. Plaintiff and the other members of the Class and New York Subclass are now deprived of the choice as to how to spend their valuable free hours and seek remuneration for the loss of valuable time as another element of damages.

59. It is well recognized victims and potential victims of identity theft incur substantial losses of personal time once faced with a data breach and the need to protect themselves. Indeed, as far back as 2007, when the U.S. Government Accountability Office ("GAO") released a report in 2007 regarding data breaches, GAO found that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[21]

60. As another element of damages, Plaintiff and the other members of the Class and New York Subclass seek a sum of money sufficient to provide them with identity theft protection services for their respective lifetimes.

61. PJ&A and Crouse had and continue to have obligations created by HIPAA, reasonable industry standards, common law, state statutory law, and Crouse's own assurances and representations to keep Plaintiff and the Class and New York Subclass's Private Information confidential and to protect such Private Information from unauthorized access.

[21] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf.

62. PJ&A's Notice letter, as well as the notice on Crouse's website,[22] both omit the size and scope of the Data Breach.

63. Plaintiff and the Class and New York Subclass have no idea how the Data Breach occurred and whether any meaningful steps are being taken to further protect and secure their Personal Information going forward. Plaintiff and the Class and New York Subclass are left to speculate as to the full impact of the Data Breach and how exactly PJ&A and Crouse intend to enhance their information security systems and monitoring capabilities to prevent further breaches.

Crouse and PJ&A Failed to Comply with Industry and Regulatory Standards

64. Because of the value of PII and PHI to hackers and identity thieves, companies in the business of storing, maintaining, and securing Private Information, such as Crouse and PJ&A, have been identified as being particularly vulnerable to cyber-attacks. Cybersecurity firms have promulgated a series of best practices that, at minimum, should be implemented by sector participants, including, but not limited to: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

65. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[23] The guidelines note businesses should protect the personal customer and consumer

[22] *See* https://www.crouse.org/news/statement-pja-data-breach/ (last accessed on June 7, 2024).

[23] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[24] The guidelines provide that "[a] sound data security plan is built on 5 key principles:"

> 1. TAKE STOCK.
> Know what personal information you have in your files and on your computers.
>
> 2. SCALE DOWN.
> Keep only what you need for your business.
>
> 3. LOCK IT.
> Protect the information that you keep.
>
> 4. PITCH IT.
> Properly dispose of what you no longer need.
>
> 5. PLAN AHEAD.
> Create a plan to respond to security incidents.[25]

66. Defendants failed to meet these basic guidelines propagated nearly a decade ago.

67. Indeed, The FTC recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

[24] *Id.*

[25] *Id.*

suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[26]

68. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

69. Crouse and PJ&A's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Crouse and PJ&A Violated HIPAA

70. As Crouse recognizes in documents maintained on its website, Crouse and PJ&A must comply with HIPAA.[27] HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[28]

---

[26] *See Start with Security*, FTC, https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last accessed on June 7, 2024).

[27] *See, e.g.*, https://www.crouse.org/wp-content/uploads/2018/03/Notice-of-PrivacyREV09-13.pdf; https://www.crouse.org/wp-content/uploads/2023/06/Corporate-Compliance-Handbook.pdf; https://www.crouse.org/wp-content/uploads/2023/02/HIPAA-Business-Associates-Uses-and-Disclosures-Polilcy.pdf; https://www.crouse.org/wp-content/uploads/2024/05/HIPAA-Business-Associates-Uses-and-Disclosures-Policy.pdf; https://www.crouse.org/wp-content/uploads/2024/05/HIPAA-Information-System-Activity-Review-Policy.pdf

[28] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

71. The Data Breach itself resulted from a combination of inadequacies demonstrating that Defendants failed to comply with safeguards mandated by HIPAA. Indeed, among other things, PJ&A's computer systems failed to:

a. Ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Ensure compliance with HIPAA security standards by Crouse and PJ&A's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

f. Identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

g. Effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. §§ 164.308(a)(5) and 164.530(b);

h. Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons

or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1); and

i. Design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

72. Crouse's security failures include preventing its HIPAA Business Associate PJ&A's failures outlined above.

73. The Data Breach resulted from a combination of insufficiencies that demonstrate Crouse and PJ&A failed to comply with safeguards mandated by HIPAA regulations.

Plaintiff and the Class and New York Subclass's Injuries and Damages

74. Plaintiff and the other members of the Class and New York Subclass are clients/patients of Crouse and its subsidiaries.

75. Plaintiff and the other members of the Class and New York Subclass provided valuable consideration (directly or indirectly)–including monies, PHI, and PII–to Crouse and its subsidiaries in exchange for certain services. A portion of said consideration (and the profits derived from such) was intended to have been used by Crouse for data security measures to secure Plaintiff and the Class and New York Subclass's Private Information.

76. As a prerequisite of receiving treatment and/or services, Plaintiff and the other members of the Class and New York Subclass had to disclose their Private Information to Crouse. In turn, Crouse and its Business Associates, including PJ&A, had a duty to secure and safeguard that Private Information.

77. Plaintiff and the other members of the Class and New York Subclass's Private Information was compromised as a direct and proximate result of the Data Breach.

78. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class and New York Subclass members have been placed at an imminent and continuing increased risk of harm from fraud and identity theft.

79. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class and New York Subclass members have been forced to expend time dealing with the effects of the Data Breach.

80. Plaintiff and the other Class and New York Subclass members face substantial risk of out-of-pocket fraud losses such as medical services billed in their names, tax return fraud, financial accounts opened in their name, and similar identity theft.

81. Plaintiff and the other Class and New York Subclass members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff.

82. Plaintiff and the other Class and New York Subclass members will incur out-of-pocket costs for protective measures such as on-going credit monitoring fees and may also incur additional costs for credit report fees, credit freeze fees, and similar costs directly related to the Data Breach.

83. Plaintiff and the other Class and New York Subclass members also suffered a loss of value of their Private Information when it was removed and acquired by cyber thieves in the Data Breach.

84. Plaintiff and the other Class and New York Subclass members have spent and will continue to spend significant amounts of time to respond to the Data Breach and monitor their financial and/or medical accounts and records for misuse.

85. Moreover, Plaintiff and the other Class and New York Subclass members have an interest in ensuring that their Private Information, which remains in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing Plaintiff and the other Class and New York Subclass members' data is not accessible online and that access to such data is limited and secured.

86. Indeed, as a result of Defendants' failure to safeguard Plaintiff and the Class and New York Subclass's Private Information, Plaintiff and the other Class and New York Subclass members are forced to live with the knowledge that their Private Information—which contains private and personal details of their life—may be disclosed to the entire world, thereby making them vulnerable to cybercriminals, permanently subjecting them to loss of security, and depriving Plaintiff and the other Class and New York Subclass members of their fundamental right to privacy.

87. As demonstrated by the statistics issued by the HSS on October 31, 2023, and outlined *supra*,[29] PII and PHI is being increasingly stolen in data breaches. This is because PII and PHI are considered extremely valuable commodities on the black market. Indeed, according to Forbes Media LLC ("Forbes"), as of 2022 private healthcare information was the most valuable commodity on the dark web. As reported by Forbes:

> It's no secret that healthcare is the industry most plagued by data breaches. Patient data is the most valuable, making it targeted by bad actors. Reports show the value of a health record can be worth

[29] *See HHS' Office for Civil Rights Settles Ransomware Cyber-Attack Investigation* (Oct. 31, 2023), HHS, https://www.hhs.gov/about/news/2023/10/31/hhs-office-civil-rights-settles-ransomware-cyber-attack-investigation.html (last accessed on June 7, 2024).

> as much as $1,000, whereas on the dark web, a credit card number is worth $5 and Social Security numbers are worth $1.[30]

88. Charged with handling highly sensitive PII and PHI, including healthcare, financial, and insurance information, Crouse and PJ&A knew or should have known the importance of safeguarding the Private Information that was entrusted to it. Crouse and PJ&A also knew or should have known of the foreseeable consequences if their data security systems were breached. This includes the significant costs that would be imposed on Crouse's patients as a result of a breach. Crouse and PJ&A nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

89. Crouse and PJ&A's failure to properly and timely notify Plaintiff and the Class and New York Subclass of the Data Breach exacerbated Plaintiff and the other members of Class and New York Subclass's injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

90. Plaintiff brings this action on her own behalf and on behalf of all natural persons similarly situated (the "Class"). Pursuant to Fed. R. Civ. P. 23(a), (b)(3) and (c)(4), Plaintiff proposes the following nationwide Class definition, subject to amendment as appropriate:

> **Nationwide Class:** All natural persons residing in the United States whose Personally Identifiable Information ("PII") and/or Protected Health Information ("PHI") was compromised as a result of the Crouse/PJ&A Data Breach which is the subject of the Notice of Data Breach letter sent by PJ&A on or about December 8, 2023.

91. Plaintiff also proposes the following New York State Subclass:

---

[30] *Healthcare Data: The Perfect Storm*, Forbes (Jan. 14, 2022), https://www.forbes.com/sites/forbestechcouncil/2022/01/14/healthcare-data-the-perfect-storm/?sh=7c8e9cc96c88 (last accessed on June 7, 2024).

> **New York Subclass:** All natural persons residing in the State of New York whose Personally Identifiable Information ("PII") and/or Protected Health Information ("PHI") was compromised as a result of the Crouse/PJ&A Data Breach which is the subject of the Notice of Data Breach letter sent by PJ&A on or about December 8, 2023 (the "New York Subclass").

92. The Class and New York Subclass defined above are readily ascertainable from information in Crouse and PJ&A's possession. Thus, identification of members of the Class and New York Subclass will be reliable and administratively feasible.

93. Excluded from the Class and New York Subclass are Defendants; Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class and New York Subclass are members of the judiciary to whom this case is assigned, their families and members of their staff, and Plaintiff's Counsel (and their families) in this action.

94. Plaintiff and the other members of the Class and the New York Subclass satisfy the numerosity, commonality, typicality, and adequacy requirements under Rule 23 of the Federal Rules of Civil Procedure.

95. **Numerosity.** The members of the Class and New York Subclass are so numerous that joinder of all of them is impracticable. While the exact number of Class and New York Subclass members is unknown to Plaintiff at this time, based on information and belief, the Class and New York Subclass consist of at least thousands of persons whose data was compromised in the Data Breach.

96. **Commonality.** There are questions of law and fact common to Plaintiff and the Class and New York Subclass, which predominate over any questions affecting only individual

Class and New York Subclass members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff and the other Class and New York Subclass members' Private Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

c. Whether Defendants truthfully represented the nature of its security systems, including their vulnerability to hackers;

d. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

e. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

f. Whether Defendants owed a duty to Class and New York Subclass members to safeguard their Private Information;

g. Whether Defendants breached their duty to Class and New York Subclass members to safeguard their Private Information;

h. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

i. Whether the Class and New York Subclass members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants' conduct was negligent *per se*;

l. Whether Defendants' acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendants failed to provide accurate and complete notice of the Data Breach in a timely manner; and

n. Whether the Class and New York Subclass members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

97. **Typicality.** Plaintiff's claims are typical of those of the other Class and New York Subclass members because Plaintiff's Private Information, like that of every other Class and New York Subclass member, was compromised in the Data Breach.

98. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class and New York Subclass. Plaintiff's Counsel are competent and experienced in litigating class actions.

99. **Predominance.** Defendants have engaged in a common course of conduct toward Plaintiff and the other Class and New York Subclass members in that Plaintiff and the other Class and New York Subclass members' data at issue here was stored on the same computer systems and allowed to be unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class and New York Subclass members, as described *supra*, predominate over any individualized issues. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

100. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class and New York Subclass members would find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class and New York Subclass members would create a risk of inconsistent or varying adjudications with respect to individual Class and New York Subclass members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class and New York Subclass member.

101. Defendants have acted on grounds that apply generally to the Class and New York Subclass as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

102. Adequate notice can be given to members of the Class and New York Subclass directly using information maintained in Defendants' records.

103. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above.

CAUSES OF ACTION

COUNT I

NEGLIGENCE
(On Behalf of Plaintiff and the Class and New York Subclass Against All Defendants)

104. Plaintiff repeats the allegations contained in paragraphs 1 through 103 as if fully alleged herein.

105. Plaintiff brings this Count on behalf of herself and the Class and New York Subclass against all Defendants.

106. Defendants had duties of care to use reasonable means to: (i) secure and safeguard their computer systems and (ii) ensure the computer systems of their Business Associates, as defined under HIPAA, were safe and secure so that Plaintiff and the other members of the Class and New York Subclass's Private Information held within those computer systems were safe and secure. This duty was to prevent disclosure of the Private Information and to safeguard the Private Information from cyber theft. Defendants' duties included a responsibility to implement processes by which they could detect and prevent a breach of their security systems in a reasonably expeditious manner and to give prompt notice to those affected by a data breach.

107. Defendants owed a duty of care to Plaintiff and the other members of the Class and New York Subclass to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, the system and networks of their Business Associates, and the personnel responsible for those systems and networks, adequately protected and safeguarded Plaintiff and the Class and New York Subclass's Private Information.

108. Defendants had a specific duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

109. Defendants owed a duty of care to Plaintiff and the other members of the Class and New York Subclass as a result of the foreseeability of cyber theft, particularly in the healthcare industry. Due to the ongoing threat and highly publicized cyber theft on businesses like Crouse and PJ&A that acquire and store Private Information, Defendants were on notice of the substantial and foreseeable risk of a cyber-attack on their computer systems and the computer systems of their Business Associates. Furthermore, it was foreseeable that Plaintiff and the other members of the Class and New York Subclass would be harmed if Crouse and PJ&A did not protect Plaintiff and the other members of the Class and New York Subclass's Private Information from cyber theft.

110. Crouse and PJ&A knew or should have known that PJ&A's systems were vulnerable to unauthorized access and exfiltration by unauthorized third parties. Crouse and PJ&A knew, or should have known, of the importance of safeguarding Plaintiff and other members of the Class and New York Subclass's Private Information.

111. Crouse and PJ&A further knew or should have known of the foreseeable consequences and harm to Plaintiff and Class and New York Subclass members, if PJ&A's data security system and network were breached – including, specifically, the risk of identity theft and related costs imposed on Plaintiff and Class and New York Subclass members as a result of a data breach. Crouse and PJ&A knew or should have known about these risk and dangers to Plaintiff and the Class and New York Subclass and taken steps to strengthen PJ&A's data, information technology, and email handling systems accordingly.

112. Crouse's duty to use reasonable data security measures arose as a result of the special relationship that existed between Crouse and Plaintiff and the other members of the Class and New York Subclass. The special relationship arose because Crouse received Plaintiff and other members of the Class and New York Subclass's confidential data as part its provision of medical services to Plaintiff and other members of the Class and New York Subclass. PJ&A, Crouse's Business Associate as defined by HIPAA, received Plaintiff and the other members of the Class and New York Subclass's Private Information from Crouse. As a result, Crouse had a duty to ensure that it had sufficient safeguards to protect against the harm to Plaintiff and the Class and New York Subclass that would result from a data breach.

113. Crouse and PJ&A breached their respective common law and statutory duties by failing to provide data security consistent with industry standards to ensure that PJ&A's systems and networks adequately protected the PII and PHI they had been entrusted against foreseeable cybercrimes. Crouse and PJ&A did not use reasonable security procedures and practices appropriate for the nature of the sensitive information PJ&A was maintaining, causing Plaintiff and other members of Class and New York Subclass's PII and PHI to be exposed. As a result,

Crouse and PJ&A increased the risk to Plaintiff and other members of the Class and New York Subclass that their PII and PHI would be compromised and stolen in a cybercrime.

114. Plaintiff and other members of Class and New York Subclass's Private Information would not have been compromised in the Data Breach but for Defendants' wrongful and negligent breach of their duties.

115. Neither Plaintiff nor, upon information and belief, the other members of the Class and New York Subclass contributed to the Data Breach or subsequent misuse of their Private Information as described in this Complaint.

116. Defendants breached their obligations to Plaintiff and the other members of the Class and New York Subclass and were otherwise negligent and reckless because they failed to properly maintain and safeguard PJ&A's computer systems and data. Upon information and belief, Defendants could have prevented this Data Breach by encrypting, or adequately encrypting, or otherwise protecting their equipment and computer files containing Plaintiff and the Class and New York Subclass's Private Information.

117. Upon information and belief, Defendants' negligent conduct also includes, but is not limited to, one or more of the following acts and omissions:

a. Failing to enact adequate privacy and security measures to protect Plaintiff and the Class and New York Subclass's Private Information from unauthorized disclosure;

b. Failing to identify foreseeable privacy and security risks, remediate those identified risks, and adequately improve privacy and security measures;

c. Failing to adequately train employees to protect consumers' Private Information;

d. Failing to adequately monitor, evaluate, and ensure the security of PJ&A's network and systems;

e. Failing to properly monitor PJ&A's data security systems for existing intrusions;

f. Failing to comply with FTC guidelines for cybersecurity, in violation of the FTC Act, 15 U.S.C. § 45;

g. Failing to adhere to industry standards for cybersecurity;

h. Failing to encrypt or adequately encrypt the Private Information;

i. Failing to implement reasonable data retention policies; and

j. Failing to disclose the Data Breach to Plaintiff and the Class and New York Subclass in a timely and accurate manner.

118. Furthermore, PJ&A was plainly aware that it should destroy any Private Information that it no longer needed to provide administrative services to its former clients, or at least should have ensured extra precautions were taken to secure such Private Information since, under such circumstances, there was effectively no longer a "legitimate business 'need to know'" for accessing it.

119. As a direct and proximate result of Defendants' negligent acts and/or omissions, Plaintiff and other members of the Class and New York Subclass's Private Information was compromised, and they are all at a high risk of identity theft and financial fraud for many years to come. Plaintiff and other members of the Class and New York Subclass Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the risk of future identity theft; (b) loss of time and loss of productivity incurred mitigating the risk of future identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) deprivation of value of Private Information; and (f) the continued risk to their Private Information, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to

undertake appropriate and adequate measures to protect Plaintiff and other members of the Class and New York Subclass's sensitive information.

120. Plaintiff seeks to remedy these harms, and to prevent the future occurrence of an additional data breach, on behalf of herself and all similarly situated persons whose Private Information were compromised as a result of the Data Breach. Plaintiff seeks compensatory damages for loss of time, opportunity costs, out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems and protocols, future annual audits, and adequate credit monitoring services funded by Defendants.

121. Accordingly, Plaintiff, individually and on behalf of all those similarly situated, seeks an Order awarding damages in an amount to be determined at trial.

COUNT II

NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class and New York Subclass Against All Defendants)

122. Plaintiff repeats the allegations contained in paragraphs 1 through 103 as if fully alleged herein.

123. Plaintiff brings this Count on behalf of herself and the Class and New York Subclass against all Defendants.

124. The FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Private Information. 15 U.S.C. § 45(a)(1).

125. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

126. Defendants violated the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving companies as large as PJ&A, including, specifically, the immense damages that would result to Plaintiff and other members of the Class and New York Subclass.

127. Defendants' violations of the FTC Act, as interpreted by the FTC to include a duty to employ adequate and reasonable data security measures, constitute negligence *per se*.

128. Plaintiff and other members of the Class and New York Subclass are within the class of persons that the FTC Act was intended to protect.

129. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and other members of the Class and New York Subclass.

130. Additionally, Crouse is an entity and PJ&A is a Business Associate covered by HIPAA (45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

131. HIPAA requires Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative,

technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). HIPAA also requires covered entities' Business Associates to appropriately safeguard the protected health information they receive or create on behalf of covered entities. 45 C.F.R. §§ 164.502(e), 164.504(e), 164.532(d)-(e). The PII and PHI at issue in this case constitutes "protected health information" within the meaning of HIPAA.

132. HIPAA further requires Defendants to disclose the unauthorized access and theft of Plaintiff and other members of the Class and New York Subclass's PII and PHI "without unreasonable delay" so that Plaintiff and Class and New York Subclass members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII and PHI. *See* 45 C.F.R. §§ 164.404, 164.406, 164.410.

133. Defendants violated HIPAA by failing to reasonably protect Plaintiff and the Class and New York Subclass's PII and PHI, as described herein.

134. Defendants' violations of HIPAA constitute negligence *per se*.

135. Plaintiff and the other members of the Class and New York Subclass are within the class of persons that HIPAA was intended to protect.

136. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

137. As a direct and proximate result of Defendants' negligent *per se* acts and/or omissions, Plaintiff and the other Class and New York Subclass members' PII and PHI was compromised, and they are all at a high risk of identity theft and financial fraud for many years to come. Plaintiff and the other members of the Class and New York Subclass have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the risk of future identity theft; (b) loss of time and loss of productivity incurred

mitigating the risk of future identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) deprivation of value of PII and PHI; and (f) the continued risk to their PII and PHI, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff and other members of the Class and New York Subclass's PII and PHI.

138. Plaintiff seeks to remedy these harms, and to prevent the future occurrence of an additional data breach, on behalf of herself and all similarly situated persons whose PII and PHI were compromised as a result of the Data Breach. Plaintiff seeks compensatory damages for loss of time, opportunity costs, out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems and protocols, future annual audits, and adequate credit monitoring services funded by Defendants.

139. Accordingly, Plaintiff, individually and on behalf of all those similarly situated, seeks an Order awarding damages in an amount to be determined at trial.

COUNT III

BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class and New York Subclass Against Defendant Crouse)

140. Plaintiff repeats the allegations contained in paragraphs 1 through 103 as if fully alleged herein.

141. Plaintiff brings this Count on behalf of herself and the Class and New York Subclass against Defendant Crouse.

142. Plaintiff and the other Class and New York Subclass members gave Crouse their Private Information in confidence, believing that Crouse would protect that information. Plaintiff and the other Class and New York Subclass members would not have provided Crouse with this

information had they known it would not be adequately protected. Crouse's acceptance and storage of Plaintiff and the other Class and New York Subclass members' Private Information created a fiduciary relationship between Crouse, on the one hand, and Plaintiff and the other Class and New York Subclass members, on the other hand. In light of this relationship, Crouse must act primarily for the benefit of their patients, which includes safeguarding and protecting Plaintiff and the other Class and New York Subclass members' Private Information.

143. Due to the nature of the relationship between Crouse, on the one hand, and Plaintiff and the other Class and New York Subclass members, on the other hand, Plaintiff and the other Class and New York Subclass members were entirely reliant upon Crouse to ensure that their Private Information was adequately protected. Plaintiff and the other Class and New York Subclass members had no way of verifying or influencing the nature and extent of Crouse's or its Business Associates' data security policies and practices. Defendant Crouse was in an exclusive position to guard against the Data Breach.

144. Crouse has a fiduciary duty to act for the benefit of Plaintiff and the other Class and New York Subclass members upon matters within the scope of their relationship. Crouse breached that duty by contracting with Business Associates that failed to properly protect the integrity of the systems containing Plaintiff and the other Class and New York Subclass members' Private Information, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff and the other Class and New York Subclass members' Private Information that Crouse collected.

145. As a direct and proximate result of Crouse's breaches of its fiduciary duties, Plaintiff and the other Class and New York Subclass members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the

compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Private Information which remains in Crouse's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data Breach; (vii) loss of potential value of their Private Information; and (viii) overpayment for the services that were received without adequate data security.

COUNT IV

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class and New York Subclass Against Defendant Crouse)

146. Plaintiff repeats the allegations contained in paragraphs 1 through 103 as if fully alleged herein.

147. Plaintiff brings this Count on behalf of herself and the Class and New York Subclass against Defendant Crouse.

148. When Plaintiff and the other Class and New York Subclass members provided their Private Information to Defendant Crouse to obtain the services provided by Crouse, they entered into implied contracts with Crouse pursuant to which Crouse agreed to reasonably protect such information.

149. Crouse solicited and invited Class and New York Subclass members to provide their Private Information as part of Crouse's regular business practices, including through its Privacy Policy. Plaintiff and the other Class and New York Subclass members accepted Crouse's offers and provided their data to Crouse.

150. In entering into such implied contracts, Plaintiff and the other Class and New York Subclass members reasonably believed and expected that Crouse's data security practices complied with relevant laws and regulations and were consistent with industry standards.

151. Plaintiff and the other Class and New York Subclass members made payments to Crouse, at least a part of which was conferred upon Crouse. Plaintiff reasonably believed and expected that Crouse would use part of those funds to maintain adequate data security. Crouse failed to do so.

152. Plaintiff and the other Class and New York Subclass members would not have entrusted their Private Information to Crouse in the absence of the implied contract between them and Crouse to keep that information secure. Plaintiff and the other Class and New York Subclass members would not have entrusted their Private Information to Crouse in the absence of its implied promise to monitor its computer systems and networks and those of its Business Associates to ensure that it adopted reasonable data security measures.

153. Plaintiff and the other Class and New York Subclass members fully and adequately performed their obligations under the implied contracts with Crouse.

154. Crouse breached its implied contracts with Plaintiff and the other Class and New York Subclass members by failing to safeguard and protect their data.

155. As a direct and proximate result of Crouse's breaches of the implied contracts, Plaintiff and the other Class and New York Subclass members sustained damages as alleged herein.

156. Plaintiff and the other Class and New York Subclass members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

157. Plaintiff and the other Class and New York Subclass members are also entitled to injunctive relief requiring Crouse to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class and New York Subclass members.

COUNT V

UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class and New York Subclass Against All Defendants)

158. Plaintiff repeats the allegations contained in paragraphs 1 through 103 as if fully alleged herein.

159. Plaintiff brings this Count on behalf of herself and the Class and New York Subclass against all Defendants.

160. Plaintiff and the Class and New York Subclass members have an interest, both equitable and legal, in the Private Information about them that was conferred upon, collected by, and maintained by Defendants and that was ultimately stolen in the Data Breach.

161. Defendants were benefitted by the conferral upon it of the Private Information pertaining to Plaintiff and Class and New York Subclass members and by its ability to retain and use that information. Defendants understood that they were in fact so benefitted.

162. Defendants also understood and appreciated that the Private Information pertaining to Plaintiff and Class and New York Subclass members was private and confidential and its value depended upon Defendants maintaining the privacy and confidentiality of that Private Information.

163. But for Defendants' willingness and commitment to maintain its privacy and confidentiality, that Private Information would not have been transferred to and entrusted with Defendants. Further, if Defendants had disclosed that its data security measures were inadequate,

Defendants would not have been permitted to continue in operation by regulators and participants in the marketplace.

164. As a result of Defendants' wrongful conduct as alleged in this Complaint (including among things thier utter failure to employ adequate data security measures, their continued maintenance and use of the Private Information belonging to Plaintiff and Class and New York Subclass members without having adequate data security measures, and their other conduct facilitating the theft of that Private Information), Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class and New York Subclass members. Among other things, Defendants continue to benefit and profit from the Private Information while its value to Plaintiff and Class and New York Subclass members has been diminished.

165. Defendants' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff and Class and New York Subclass members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

166. Under the common law doctrine of unjust enrichment, it is inequitable for Defendants to be permitted to retain the benefits they received, and are still receiving, without justification, from Plaintiff and Class and New York Subclass members in an unfair and unconscionable manner. Defendants' retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

167. The benefit conferred upon, received, and enjoyed by Defendants was not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendants to retain the benefit.

168. Defendants are therefore liable to Plaintiff and Class and New York Subclass members for restitution in the amount of the benefit conferred on Defendants as a result of their wrongful conduct, including specifically the value to Defendants of the Private Information that was stolen in the Breach and the profits Defendants are receiving from the use of that information.

COUNT VI

VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 349
(On Behalf of Plaintiff and the Class and New York Subclass Against Defendant Crouse)

169. Plaintiff repeats the allegations contained in paragraphs 1 through 103 as if fully alleged herein.

170. Plaintiff brings this Count on behalf of herself and the Class and New York Subclass against Defendant Crouse.

171. Crouse, while operating in the State of New York, engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to enact adequate privacy and security measures to protect Plaintiff and the Class and New York Subclass's Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable privacy and security risks, remediate those identified risks, and adequately improve privacy and security measures, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the privacy and security of Plaintiff and the Class and New York Subclass's Private Information, including, but not limited to, duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and the Class and New York Subclass's Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the Class and New York Subclass's Private Information, including, but not limited to, duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d;

f. Failing to disclose the Data Breach to Plaintiff and the Class and New York Subclass in a timely and accurate manner;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and the Class and New York Subclass's Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the Class and New York Subclass's Private Information, including, but not limited to, duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d.

172. Crouse's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Crouse and its vendors' data security and ability to protect the confidentiality of patients' PII and PHI.

173. Crouse's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and other members of the Class and New York Subclass, that their PII and PHI would not and had not been exposed and misled Plaintiff and other members of the Class and New York Subclass into believing they did not need to take actions to secure their identities.

174. Crouse acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and other members of the Class and New York Subclass's rights.

175. As a direct and proximate result of Crouse's deceptive and unlawful acts and practices, Plaintiff and other members of the Class and New York Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-

monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII and PHI.

176. Crouse's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, particularly the New Yorkers directly affected by the Data Breach.

177. The above deceptive and unlawful practices and acts by Crouse caused substantial injury to Plaintiff and other members of the Class and New York subclass that they could not reasonably avoid.

178. Plaintiff and other members of the Class and New York Sublass seek all monetary and non-monetary relief allowed by law, including actual damages treble damages, injunctive relief, and attorney's fees and costs.

PRAYER FOR RELIEF

WHEREFORE Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her Counsel to represent the Class and New York Subclass;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff and the other Class and New York Subclass members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and the other Class and New York Subclass members or to mitigate further harm;

C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to

disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

E. Ordering Defendants to pay for not less than seven years of credit monitoring services for Plaintiff and the proposed Class and New York Subclass;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including reasonable expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff hereby demands a jury trial for all claims so triable.

DATED: June 17, 2024

Respectfully submitted,

ABRAHAM, FRUCHTER
& TWERSKY, LLP

/s/ Mitchell M.Z. Twersky
Mitchell M.Z. Twersky
450 Seventh Avenue, 38th Floor
New York NY 10123
Tel: 212-279-5050
Fax: 212-279-3655
Email: mtwersky@aftlaw.com

Patrice L. Bishop
ABRAHAM, FRUCHTER
& TWERSKY, LLP
9440 Santa Monica Blvd.
Bank of America Building
Suite 301
Beverly Hills, CA 90210
Tel: 310-279-5125
Email: pbishop@aftlaw.com

Jean Martin
MORGAN & MORGAN, P.A.
201 N Franklin St, 7th Floor,
Tampa, FL 33602
Tel: 813-559-4908
Fax: 813-222-4795
Email: jeanmartin@forthepeople.com

Attorneys for Plaintiff